Rapport sur les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) face aux développements technologiques (partie I)

Dinant, Jean-Marc

Publication date:
2010

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 5 November 2010 T-PD-BUR(2010)09 (I) FINAL

LE BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNES A CARACTERE PERSONNEL

(T-PD-BUR)

22ème réunion
15-17 novembre 2010
Strasbourg, salle G04

Rapport sur les lacunes de la Convention n°108 pou r la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques

(Partie I)

CENTRE DE RECHERCHES INFORMATIQUE ET DROIT

Auteur :

Jean-Marc Dinant,

Docteur en informatique

Directeur de recherche au Centre de Recherche Informatique et Droit

Expert judiciaire

Document du Secrétariat preparé par
la Direction Générale des affaires juridiques et des droits de l'Homme

TABLE DES MATIERES

1. Des nouveaux micro réseaux de télécommunication

La première décennie du 21ème siècle a vu se diffuser à une vitesse sans cesse croissante de nouveaux réseaux de télécommunication, tandis que la croissance du réseau Internet, tant en termes de rapidité que de mobilité et d'ubiquité, continuait à un rythme soutenu, du moins dans les pays développés.

Divers réseaux sans fil à courte portée (entre quelques centimètres et quelques dizaines de mètres et que nous appellerons dans ce qui suit "micro réseaux"), principalement les réseaux de type Wifi, RFID et BlueTooth, se sont récemment développés sans grande précaution par rapport à la protection des données et de la vie privée de leurs utilisateurs.
Les interfaces Wifi sont aujourd'hui généralisées dans les ordinateurs portables et équipent progressivement les téléphones mobiles. Il y a en pratique une convergence entre les « laptop » et les téléphones mobiles. Les premiers permettent de plus en plus la téléphonie grâce à des applications de VoIP comme Skype. Les seconds permettent de plus en plus à leur utilisateur, non seulement de téléphoner, mais aussi de surfer, de recevoir et d'envoyer des courriels ou même d'accéder aux réseaux sociaux via le réseau Internet. Ces réseaux représentent aujourd'hui une menace majeure et insuffisamment prise en compte par rapport à la traçabilité des utilisateurs, ou, plus largement par rapport aux êtres humains porteurs de ces terminaux connectés à ces nouveaux réseaux de télécommunication. Ces risques peuvent être synthétisés comme suit :

- Perte de contrôle : l'absence d'une connexion physique de type filaire pour ces nouveaux réseaux rend leur déconnection problématique et leur fonctionnement invisible même pour un utilisateur averti. Ce problème est particulièrement gênant pour les puces RFID qui fonctionnent sans batterie et dont la taille minuscule, de l'ordre de quelques millimètres, n'aide pas l'utilisateur à détecter leur présence. Comme ces puces sont notamment utilisées pour la lutte contre le vol dans les magasins, ces derniers n'ont évidemment pas d'intérêt à rendre ces puces visibles dans la mesure où un voleur potentiel pourrait les arracher ou les endommager.

- Absence de confidentialité : les trois réseaux précités ne sont pas chiffrés systématiquement. En particulier en ce qui concerne le réseau Wifi, il est relativement facile pour un tiers de capter et de lire le trafic entre un terminal sans fil et la borne Wifi

- Possibilité de traçabilité : Même lorsque les communications sont chiffrés, le numéro de série électronique statique qui équipe une borne Wifi, une puce RFID ou un mobile BlueTooth demeure généralement lisible en clair. Ces appareils sont de type serveur, c-à-d que, techniquement, ils répondent automatiquement à une tentative de connexion, même si elle est abusive et non suivie d'effet, en communiquant leur numéro de série électronique unique au monde (GUID = Global Unique Identifier). En général, il est donc techniquement possible de lire un numéro de série BlueTooth, l'adresse MAC d'une carte WiFi ou le numéro de série d'une puce RFID, même sans entamer une véritable communication

En conclusion, ces nouveaux réseaux largement disséminés et dont la croissance sera exponentielle durant les années à venir, permettent de manière technique et invisible le suivi individuel de chaque terminal équipé d'une interface WiFi, RFID ou BlueTooth, à l'insu de son détenteur, même lorsque l'équipement terminal n'est pas volontairement activé.

2. L'explosion de la géolocalisation

La captation d'un numéro de série d'un terminal sans fil peut s'opérer par le biais d'un ordinateur équipé de capacités de géo localisation, typiquement d'un système GPS1. Comme ces nouveaux micro réseaux sont de plus en plus reliés à des terminaux aussi sont eux-mêmes reliés au réseau Internet, l'adresse Ipv4 dynamique qui se renouvelle aléatoirement et de manière régulière ne procure plus de protection efficace contre la traçabilité des utilisateurs de réseaux de télécommunication. En effet, il est souvent possible d'identifier un numéro de série ou un tag unique propre au micro réseau utilisé. La fusion de ces micro réseaux avec le réseau global Internet conduit de manière silencieuse et inéluctable à un suivi de plus en plus systématique de la localisation des individus.

Il faut analyser les risques de cette géo localisation de manière globale. Il s'agit bien plus que de savoir où un individu se trouve à un moment donné :

- Ce système appliqué à une part importante de la population permet de savoir **avec qui** une personne déterminée se trouve et d'ainsi pouvoir dresser une cartographie des relations familiales, professionnelles ou amicales de chaque personne.

- De nombreux lieux sont empreints d'une signification particulière. La connaissance se situe bien au delà de la simple information. Le numéro 25 de la rue principale d'une grande ville n'est a priori pas très significatif, sauf si l'on sait qu'il s'agit d'une mosquée, d'un hôpital psychiatrique, d'un local syndical, d'un commissariat de police ou d'un tribunal.

- Les trajectoires d'un individu sont typiques d'un certain type de comportement. Il est ainsi possible de savoir si une personne s'arrête devant une vitrine ou si elle fait du jogging. A l'intérieur d'un grand magasin, les trajectoires des individus sont représentatives de comportement d'achat.

Cette géo localisation peut en outre se coupler avec la surveillance systématique du comportement en ligne des utilisateurs que nous avons décrite précédemment2. Le couplage des deux systèmes (profilage en ligne et géo localisation) est techniquement facilité par l'interconnexion des micros réseaux de géo localisation avec le terminal utilisé pour se connecter à Internet.

---

[1] Le système GPS est purement passif : une puce GPS capte des signaux issus de satellites géostationnaires situés à plusieurs dizaines de milliers de kilomètres et n'émet aucun signal. La puce calcule en permanence la distance qui la sépare des satellites dont elle connaît la position et calcule, par triangulation, sa position exacte (à quelques mètres près). Les problèmes de privacy ne sont pas liés au GPS lui-même mais au stockage et à la transmission des données de géo localisation par le terminal incorporant cette puce GPS.

[2] Poullet, Yves & Dinant Jean-Marc**Report on the application of data protection principles to the worldwide telecommunication networks***Information self-determination in the internet era*Rapport d'expertise à l'attention du Conseil de l'Europe, Strasbourg, 2004 http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/

3. L'invasion des cookies ou la disparition de l'intraçabilité

Les cookies ont été construits afin de permettre la traçabilité des utilisateurs du Web, nonobstant le changement d'adresse IP ou le partage d'une même adresse entre plusieurs utilisateurs3. Cette traçabilité peut être nécessaire pour les transactions électronique en ligne mais, techniquement, seuls les cookies de session directs se justifient pour cette finalité. Or, ce qui pose aujourd'hui problème, ce sont les cookies rémanents ou les cookies de tierces parties et, corollairement les cookies rémanents de tierces parties qui surveillent le trafic par transclusivité. Dans ce registre, le champion du monde en titre est indiscutablement Google qui grâce à son système Google Analytics collecte en permanence le trafic (les URL et donc le contenu) le trafic sur la majorité des sites Internet4.

Toutefois, jusqu'il y a peu, un paramétrage du navigateur permettait à l'utilisateur averti de bloquer les cookies tierces parties. Il est à souligner qu'aucun navigateur classique ne permet de bloquer la transclusivité (c-à-d l'incorporation automatique de contenus par des sites tiers inconnus de l'internaute (contactibilité) et la communication des données de trafic à ces mêmes sites tiers (observabilité)). Le blocage des cookies rémanents tierce partie agit uniquement sur la traçabilité. Deux éléments importants ont remis en cause ce contrôle marginal de la traçabilité.

La première remise en cause de cette possibilité que possède l'utilisateur averti de bloquer les cookies au niveau du protocole HTTP du WEB a été provoquée par l'apparition des cookies FLASH. Macromedia diffuse à une échelle mondiale la technologie FLASH sous forme de plug-in qui est installé sur les navigateurs les plus courants. Ce plug-in possède un fonctionnement propre et un système de gestion de données indépendant qui peut être utilisé comme un système de cookies. Dans ce cas, le blocage opéré par le navigateur se relève totalement inopérant. Il est possible pour l'utilisateur expert de trouver une parade à ce comportement étrange du plug-in qui possède donc cette capacité de lire et d'écrire des données sur la mémoire de masse du terminal. Toutefois, comme les cookies Flash sont peu connus et comme la démarche de blocage nécessite des connaissances techniques approfondies, ce type de blocage est peu utilisé.

Une deuxième phénomène remet en cause ce blocage des cookies tierces-partie par l'utilisateur averti. Pour les téléphones mobiles en général et pour l'Iphone d'Apple en particulier, il existe une tendance pour les sites web importants de développer leur propre application. Alors que leur site pourrait être utilisé via un navigateur classique de type Firefox, de nombreuses sociétés (Amazon, FaceBook, Google, certains journaux) développent et distribuent leur propre application. Cette application utilise le protocole HTTP mais l'utilisateur ne possède plus la possibilité de bloquer les cookies et encore moins la transclusivité.

Dans la même lignée, l'incorporation systématique de l'adresse MAC5 dans l'adresse IP version 6 (Ipv6) augmente(ra) de manière importante et en catimini les capacités de traçabilité des surfeurs sur les sites Web. Malgré un changement d'adresse IP et contrairement à l'actuel protocole IP version 4 (Ipv4), chaque adresse Ipv6 contiendra le numéro de série unique de la carte réseau de l'ordinateur. Ce risque, bien plus grand que les cookies rémanents de tierces parties, demeure actuellement

[3] Système NAT présent sur la plupart des bornes Wifi et des routeur ADSL domestiques qui permet à plusieurs utilisateurs distincts d'utiliser simultanément une même adresse IP sur Internet

[4] Etude de Berkeley portant sur un échantillion de 400.000 sites en mai 2009 et montrant que 88% d'entre eux utililisent Google Analytics

[5] Medium Access Control. Numéro de série unique au niveau mondial de chaque périphérique Ethernet comme par exemple, les carte et les bornes Wifi, les cartes réseau. Les puces Bluetooth rproduisent souvent ne numéro de série de la carte Ethernet de l'appareil surlequel elles se trouvent.

insuffisamment pris en considération par les autorités de protection des données. Un protocole IPv6 alternatif générant une adresse aléatoire existe et a été approuvé par le W3C.

De manière générale, on constate donc que les bien faibles remparts qui permettaient à l'utilisateur averti de lutter contre la traçabilité sur le réseau Internet sont en train, lentement mais sûrement, de s'éroder.

4. Les réseaux sociaux

Si à la fin du vingtième siècle, le courriel et le chat étaient les moyens de communication interpersonnelle les plus prisés sur Internet, on a vu se développer les réseaux sociaux qui sont une évolution technique naturelle des blogs d'antan. L'innovation est ici sociale : là où les blogs se concentraient sur une problématique ou un thème particulier, les réseaux sociaux se concentrent sur les individus. Rapidement, ces réseaux sociaux sont devenus une manière d'entrer en relation et de se faire connaître sur Internet. Les concepteurs de ces réseaux sociaux ont rapidement mis au point des applications spécifiques qui permettent à des tiers de parcourir ces réseaux et d'intervenir sur les profils qui y sont stockés, selon les modalités permises par les utilisateurs et par le concepteur du réseau. Ces réseaux sociaux sont généralement faussement gratuits, c-à-d que leur utilisateur rémunère le réseau social par le biais de son exposition publicitaire. Les politiques de protection de la vie privée de ces réseaux sont généralement dictées par le concepteur du site qui peut permettre aux personnes concernées de paramétrer, dans une certaine mesure qu'il détermine, la visibilité des informations stockées vis-à-vis des tiers.

Depuis toujours, les lois relatives à la protection des données à caractère personnel se sont focalisées sur le double concept de données à caractère personnel et de "maître du fichier" ou "responsable du traitement". Ces deux concepts semblent devenus aujourd'hui à la fois trop flous et trop étroits pour conduire à une réglementation efficace du droit au respect de la vie privée au sein des technologies et usages sans cesse changeants de la société de l'information et de la communication.

5. Une approche fonctionnelle du concept de donnée à caractère personnel

Toute donnée liée à un individu identifie généralement une caractéristique de ce dernier. Cette donnée peut être biographique et/ou traçante.

Dans le premier cas, la donnée qui se rapporte à un individu raconte quelque chose par rapport à cette personne : par exemple un fait, un geste, un parcours ou un achat ; il s'agit d'une propriété de la personne qui peut être partagée entre plusieurs individus. Par exemple, le fait d'être corse ou catalan est une donnée personnelle de chaque corse ou chaque catalan. Il s'agit d'une donnée « biographique » au sens étymologique, c-a-d une information qui (d)écrit la vie ou plus exactement une tranche de vie, une caractéristique d'un individu. L'enjeu est donc ici la **connaissance** d'une ou plusieurs caractéristiques d'un individu **dans un contexte particulier**.

Dans le deuxième cas, la donnée se rapporte à un individu et constitue une caractéristique unique ou une valeur unique de certaines variables qui le distingue de manière certaine des autres individus au sein d'une population donnée. Ainsi une adresse IP identifie une personne de manière unique à un

moment donné6. Il s'agit d'un identifiant unique (Unique Identifier). Cet identifiant n'est guère problématique lorsqu'il s'agit d'identifier un individu dans un contexte particulier (numéro de compte dans une banque, numéro de patient dans un hôpital, numéro d'étudiant dans une université, numéro de citoyen dans une administration, numéro d'affilié dans un syndicat, etc). Toutefois, en pratique, ces identifiants sont rarement locaux mais deviennent rapidement globaux, c-à-d multicontextuels. On parle alors d'Identifiant Global Unique (Global Unique Identifier). Ce type d'identifiant permet la traçabilité d'une même personne au sein de plusieurs contexte différents. L'enjeu est donc ici une **connaissance multicontextuelle** d'un même individu.

Les données contactuelles constituent un troisième type de donnée. Une adresse email, une adresse postale, l'URL d'un « mur » sur un site social permettent à un tiers de communiquer un contenu à un individu identifié par une donnée de contact. Ainsi, par exemple, la connaissance d'une adresse email pourrait permettre d'identifier plusieurs pages WEB relatives au même individu. L'enjeu de ce dernier type de donnée est la **contactabilité**, ou la possibilité techniquement offerte à un tiers d'injecter un contenu informationnel (et notamment de la publicité) dans une boîte aux lettres ou sur un écran. Dans ce contexte, c'est naturellement de marketing dont il s'agit et, plus précisément du contrôle de l'individu par rapport à son **exposition publicitaire**.

Cette division fonctionnelle des données distingue en fait trois types de données à caractère personnel qui sont substantiellement différentes. Il s'agit, plus précisément, de propriétés des données à caractère personnel. Ainsi, une adresse email de type « john.smith@coe.int » cumule les trois propriétés décrites ci-dessus. On peut savoir que John Smith travaille au Conseil de l'Europe. En tapant son adresse mail sur un moteur de recherche, on pourra trouver des informations qui y sont associées et enfin, l'adresse mail va permettre de contacter John Smith, éventuellement à des fins publicitaires

De très (trop ?) longs débats ont eu lieu depuis longtemps sur le caractère de données à caractère personnel de l'adresse IP ou des cookies. Il est à souligner que l'importance apparente de ce débat est liée à une confusion présente au sein des les entreprises, notamment multinationales. L'article 8 de la CEDH ne protège pas la vie privée de l'homme identifié ou identifiable. Toute personne même non identifiée ou identifiable a droit à cette protection. Le droit à la protection des données à caractère personnel n'épuise pas le droit à la protection de la vie privée. Ainsi, par exemple, la surveillance omniprésente des personnes dans les lieux publics ou privés par des moyens de vidéo surveillance constitue bel et bien une intrusion dans la vie des personnes filmées, quand bien même elles demeureraient non identifiables grâce à un savant floutage de leur visage.

En d'autres termes, à notre sens, il n'existe pas de donnée concernant un individu qui ne l'identifie, soit de manière traçante, soit de manière biographique ou qui ne permette de le contacter.

Il est à noter que certains de ces problèmes sont déjà pris en considération par certaines directives européennes qui ne nous semblent pas avoir d'équivalent au sein du Conseil de l'Europe. Ainsi, par exemple, la directive CE 95/46 prévoit le droit de s'opposer au marketing direct sans aucune justification. La directive CE 2002/58 réglemente l'usage qui peut être fait du courrier électronique et soumet l'utilisation de celui-ci à des fins commerciales au consentement ou à la possibilité d'exercer un droit d'opposition dans le chef de la personne concernée. La directive CE 2006/24 détermine de manière exhaustive les données de trafic qui doivent être conservées par les opérateurs de télécommunication, par dérogation à la Directive 2002/58. Etc.

---

[6] Ceci est vrai en règle générale si l'utilisateur n'utilise pas de système NAT. Dans le cas d'un système NAT permettant le partage simultané d'une même adresse IP entre plusieurs personnes (élèves d'une école, membre d'une famille, hôtes d'un hotel, etc), l'adresse IP identifiie un groupe de personnes.

Il est à relever que ces dispositions du droit communautaire européen font preuve d'un plus grand pragmatisme et prétendent protéger la vie privée et les données à caractère personnel. On peut d'ailleurs noter que la protection du courrier électronique profitera tout autant aux personnes morales qu'aux personnes physiques.

En conclusion, il est devenu de moins en moins pertinent de se poser la question de savoir si telle ou telle donnée est une donnée à caractère personnel mais plutôt d'identifier les risques que fait courir l'utilisation des données issues des technologies de l'information et la communication dans un contexte particulier par un utilisateur donné et d'y apporter une réponse de principe.

A notre sens, les données les plus sensibles sont aujourd'hui les Identifiants Globaux Uniques hardware (numéro de série électronique) ou software (cookie) dans la mesure où, étant fermement attachés à un terminal de télécommunication, ils permettent la traçabilité d'un même utilisateur dans plusieurs contextes différents. L'utilisation des ces numéros uniques devrait être restreinte au terminal. Ils ne devraient pas devoir transiter jusque dans les réseaux de télécommunication, en l'absence de garanties appropriées.

Les données de trafic devraient elles aussi jouir d'un statut particulier. En droit européen, le principe d'anonymisation ou de destruction immédiate des données de trafic est inscrit à l'article 6 de la Directive 2002/54. Par dérogation à ce principe général, les opérateurs, sur base de la directive 2006/24 sont contraints de conserver un nombre limité de données pour une période limitée et aux seules fins de la poursuite et de la recherche des infractions pénales. Il est piquant de constater que Google collecte aujourd'hui en temps réel l'ensemble des données de trafic du Web sur une base individuelle et à des fins commerciales (le marketing direct a rapporté à Google plus de six milliards de US $ en 20097) alors que semblable collecte est expressément interdite aux opérateurs de télécommunication à des fins de détection et de poursuite par les forces de police des délits criminels. Qu'en d'autres termes, un acteur puissant d'Internet collecte quotidiennement et de facto bien plus de données personnelles à des fins commerciales que ne le peuvent et ne le font les services de polices, par le biais des opérateurs, à des fins de lutte contre les atteintes à la sécurité publique.

6. Le maître du fichier

Tant la Directive 95/46 que la Convention 108 distinguent deux personnes responsables du traitement des données : le responsable du traitement (maître du fichier) et le sous-traitant.

Cette catégorisation ne nous semble plus adéquate. Le monde des TIC s'est spécialisé et de nouveaux métiers se sont créés. D'autres métiers émergeront demain.

Pour parvenir à mener à bien cette régulation, il convient d'adapter le régime légal en fonction du métier de la société qui collecte, stocke ou transmet des données relatives aux individus.
Nous avons par ailleurs bien conscience que cette régulation se heurte actuellement à un problème de Droit International Privé. A l'instar du droit de la consommation, la protection des données (qui devient un aspect de plus en plus important de ce droit de la consommation) ne devrait il pas être celui de la personne concernée et non celui de l'établissement de la société qui collecte, stocke ou transmet ces données ? Ce point sera abordé en détail dans notre deuxième partie.

---

[7] Voir à ce sujet « *Bénéfices en forte hausse pour Google* » *in « Le Monde, 16 octobre 2009, http://www.lemonde.fr/technologies/article/2009/10/16/benefices-en-forte-hausse-pour-google_1254699_651865.html*

Sous la pression populaire, certains grands acteurs (FaceBook, Google) ont parfois modifié leurs politiques en matière de vie privée mais un tel mode de régulation par essai et erreur n'apparait pas satisfaisant. Les attaques de plus en plus subtiles contre la protection des données à caractère personnel et contre la vie privé des internautes sont motivées par des considérations économiques de grands acteurs de l'Internet et génèrent, par effet de bord, des problèmes dont le coût social est porté par la société dans son ensemble.

Sur ce point précis, nous constatons que le financement de nombreux outils de la société de l'information et de la communication (moteur de recherche, réseaux sociaux, courrier électronique,…) est basé sur la publicité. L'argument clé des publicitaires, à savoir la gratuité de l'Internet, se révèle, à l'analyse, bancal. Si c'est la publicité qui finance l'internet, il faut évidemment se demander qui finance la publicité. Bien loin de recevoir un Internet gratuit, le consommateur paie en fait deux fois. Il paie tout d'abord en nature en se faisant profiler, analyser et manipuler tant dans son conscient que dans son inconscient. Le consommateur paie une deuxième fois en achetant le produit ou le service ainsi promu et dont le coût se trouve inéluctablement inclus dans le prix final.

De nombreux auteurs ont mené une réflexion sur la marchandisation de la vie privée et des données à caractère personnel. Il semble aujourd'hui acquis, que la protection de la vie privée est une liberté fondamentale. Et c'est bien parce qu'il s'agit d'une liberté fondamentale que cette vie privée peut, dans une certaine mesure et sous certaine conditions se monnayer. A l'instar du droit à l'image monnayé par les vedettes du show biz, chaque individu devrait pouvoir non seulement refuser ou accepter l'exposition publicitaire mais aussi la monnayer contre des espèces sonnantes et trébuchantes. Il serait donc souhaitable que l'accès aux services de la société de l'information et de la communication ne soit plus conditionné par une obligation de fait de se soumettre à l'analyse comportementale et à l'injection de contenus publicitaires mais puisse être payée par le consommateur via une contribution financière Ces services sans publicités pourraient être rendus accessibles aux citoyens par les fournisseurs d'accès à Internet, moyennant une modeste contribution financière et forfaitaire incluse dans le coût de l'abonnement Internet. En effet, si l'on ramène grossièrement le bénéfice de Google au nombre d'internaute concernés, on se rend compte que l'accès aux services de Google pourrait s'effectuer pour un prix d'environ un euro par internaute et par mois, sans que le bénéfice de Google en soit affecté de manière significative.

7. Une "success story" ?

A notre sens, le réseau téléphonique mobile moderne demeure un exemple à suivre en matière de protection de la vie privée intégré au cœur de la technologie. D'une part, les terminaux de téléphonie mobile doivent (sous peine de ne pas être agrées et donc impossibles à vendre) inclure le Calling Line Identification Restriction. Cette fonctionnalité permet à tout utilisateur, même néophyte, de masquer son numéro d'appel à la personne à qui elle téléphone. Techniquement, il faut savoir que ce numéro est toujours techniquement transmis, ce qui permet, par exemple aux services d'urgence, dans les conditions prévues par ou en vertu de la loi, de procéder à l'identification du numéro appelant ces services.

Les appareils téléphonique mobiles possèdent eux aussi un numéro de série électronique appelé IMEI (*International Mobile Equipment Identity)*. Ce numéro de série est transmis à l'opérateur du réseau téléphonique et à lui seul. L'opérateur du réseau ne transmet pas techniquement ce numéro de série sur l'appareil mobile du destinataire de la télécommunication. Toutefois, en vertu de la Directive 2006/24, les opérateurs doivent conserver cette donnée d'identification. Ces éléments techniques permettent à l'utilisateur un réel contrôle sur la téléphonie mobile. Il peut masquer son numéro d'appel et gère ainsi sa traçabilité et sa contactabilité. Sa communication est chiffrée et n'est pas facilement observable par un tiers.

On peut constater un certain consensus au sujet des principes de protection de la vie privée et des données à caractère personnelles (ontologie de la privacy : contrôle sur l'observabilité, la traçabilité et la contactibilité ; respect du principe de finalité (contextualisation des données)), de nombreuses recherches relatives au « privacy by design » sont en cours.

Nous pensons que face aux défis présents et à venir la loi doit s'adresser de manière différente à tous les acteurs de la société de l'information et de la communication, selon le rôle qu'ils jouent et le type de données qu'ils sont appelés à traiter. Sur les autoroutes de l'information, le code de la route ne suffit plus ; il faut produire des véhicules, de la technologie qui mette en œuvre ces principes de protection du conducteur. « If the technology is the problem, the technology may be the answer… »